[10191/1365]

A METHOD FOR ASSIGNING A REMOTE CONTROL OPERATION TO A BASE STATION

Background Information

The invention relates to a method in accordance with the species of the main claim, as described in the German Patent Application AZ: 196 45 769.6. In accordance therewith, the assignment of a remote control operation to a base station arranged in a motor vehicle takes place by the base station transmitting a search signal, in response to which the remote control operations located in the transmission range of the search signal respond by transmitting back a contact signal at time points characteristic for the remote control operations. By evaluating the entry time points of the contact signal return transmissions, the base station detects the available remote control operations. It selects one of them and carries out with it a "challenge response" verification. Because an unequivocal remote control recognition is possible through exchanging only one signal, and the signal can be designed in a simple manner because it is not security-relevant, the entire detection process proceeds very rapidly. Therefore, for the speed of assignment, it is above all the subsequent challenge-response verification that is determinative. The verification is based on carrying out security-relevant arithmetic operations, which are extensive and, accordingly, require time response signal, user-specific, integrated circuits (ASIC) specially developed for this purpose are used, which carry out the challenge or response calculation in less than three milliseconds. Thus the triggering of the assignment test can take place as a result of actuating the door handle of a motor vehicle, so that the door can only be opened if the remote control operation has been verified as belonging to the motor vehicle. The user does not notice the assignment process. The above-mentioned ASICs perform their function well, but they are comparatively expensive to manufacture.

It is the objective of the invention to indicate a method for assigning a remote control operation to a base station, the method permitting a rapid execution of an assignment test, in particular a rapid execution of a verification communication.

The objective is achieved through a method having the features of the main claim. The method according to the invention can be easily realized as a program in the microprocessor that is present in any case in the base station and in the remote control operation, making the availability of an ASIC superfluous. In this context, the method assures the same security as when an ASIC is used. Advantageously, an increase in security can be realized due to the fact that the speed of the challenge-response calculation can be controlled in a deliberate manner if the challenge-response dialog is carried out multiple times one immediately after the other.

One exemplary embodiment of the invention is discussed in greater detail below with reference to the drawing.

Drawing

Figure 1 depicts a block diagram of an access device, and Figure 2 depicts a flowchart to make clear its operation.

Description

Figure 1 depicts a base station 10, which can be a part of an apparatus or object, or which is permanently assigned to one such. For example, the base station can be a part of the access control device of a building or of a motor vehicle. A further component of the access device depicted in Figure 1 is an operating device 20 designated hereinafter as remote control operation, which is assigned to the base station functionally via a contactless signal transmission link 30. The remote control operation, in particular, can be a transponder. Via undepicted operative connections, base station 10 acts upon the technical device, to which or to a part of which, it is assigned. When used in a motor vehicle, it controls, for example, access to the vehicle or to its ignition.

A component of base station 10 is a microprocessor 13, which controls the operation of base station 10, for this purpose, in particular, prompting the transmission of signals and evaluating incoming signals. Connected to the microprocessor is a transmitting/receiving device 11 for transmitting or receiving signals that are transmitted, without contact, via signal transmission link 30. Furthermore, microprocessor 13 has assigned to it a memory 14. In it is

found assignment information, on the basis of which base station 10 recognizes assigned remote control operations 20. The assignment information is: a serial number 15, a manufacturer code 17, an encryption keycode 31, a directory 16 having information on remote control operations 20 assigned to base station 10, and a random number 18. Serial number 15 is characteristic for base stations 10 and remote control operations 20 that are assigned to each other. It is determined by the manufacturer of the technical device to which base station 10 and remote control operations 20 are assigned. For use in motor vehicles, the determination can be made by the vehicle manufacturer. Manufacturer code 17 unambiguously designates the corresponding apparatus, i.e., base station 10. It is issued by the manufacturer of the base station and is unchangeable. Directory 16 contains for every assigned remote control operation 20 a data record 16a, 16b, 16c, each of which contains group number 25 of a remote control operation 20, its manufacturer code 27, a random number, as well as a setpoint response. Group numbers 25, in this context, distinguish the remote control operations that have the same serial numbers and that are assigned to a base station 10, and manufacturer code 27, specific in each case, in connection with encryption keycode 31 and random number 18, which is generated by microprocessor 13, functions to produce the setpoint response. Encryption keycode 31 is also advantageously determined by the manufacturer of the corresponding technical device, such as a motor vehicle manufacturer. In each case, an entire data record 16a, 16b, 16c makes possible the verification of a corresponding remote control operation 20.

The remote control operation has at its disposal a transmitting/receiving device 21 corresponding to base-station-side transmitting/receiving device 11, for receiving signals transmitted by base station 10 or for transmitting signals to base station 10. By analogy to the base station, a microprocessor 23 is connected downstream of transmitting/receiving device 21, the microprocessor controlling the operation of remote control operation 20, especially undertaking the evaluation of the signals coming in via transmitting/receiving device 22, initiating subsequent measures as a function of the results, and monitoring the generation of output signals. Microprocessor 23 has assigned to it a memory unit 24, wherein assignment information is stored for assigning remote control operation 20 to a base station 10. Stored for this purpose -- by analogy to base station 10 -- are a serial number 15, a group number 25, a manufacturer code 27, as well as an encryption keycode 31. The significance of the memory contents corresponds specifically to the significance of the similar memory contents in

memory 14 of base station 10. The manufacturer code is issued by the manufacturer of remote control operation 20 and designates the latter unambiguously. Serial number 15 is a code that is characteristic for the entire device composed of base station 10 and corresponding remote control operations 20 and is identical to the serial number contained in memory 14 of base station 10. Group number 25 distinguishes remote control operations from each other having same serial number 15. The group number is determined by the user in response to the use of the entire device. Encryption keycode 31 is determined by the manufacturer of the technical device corresponding to base station 10, and it is identical to the one present in the base station. In connection with manufacturer code 27 and the challenge signal supplied by base station 10 via signal transmission link 30, the encryption keycode functions to verify the matching to a base station 10.

Between base station 10 and remote control operations 20, there exists a signal transmission link for transmitting contactless transmissible signals between remote-control-operation-side transmitting/receiving device 21 and base-station-side transmitting/receiving device 11. The signals emitted by base-station-side transmitting/receiving device 11, in this context, reach all remote control operations 20 located within their transmission range. As signals, it is expedient to use infrared or high frequency signals.

One base station 10 can have assigned to it a plurality of remote control operations 20. All remote control operations 20 and base station 10 have available to them in their memories 14, 24 an identical serial number 15 and, in the verification, make use of an encryption keycode 31. Individual remote control operations 20 are distinguished by their group numbers 25 and their manufacturer code 27.

On the basis of Figure 2, the operation of the device depicted in Figure 1 is explained. In this context, a letter B or F is placed in front of each sequence step, indicating whether the corresponding sequence step takes place in base station 10: B or in a remote control operation 20: F.

The assignment process is triggered by the actuation of an undepicted mechanical, electrical, or electro-optical triggering mechanism by a user, step 100. When used in a motor vehicle, the triggering mechanism can, specifically, entail the actuating of the door handle.

On the basis of a signal emitted in response to triggering, microprocessor 13 of base station 10 first sets an internal counter A at value 0, step 102. Then the microprocessor from a memory 14 loads random number 18, which then constitutes, for all remote control operations 20 assigned to base station 10, the activation signal, hereinafter termed the "challenge" signal, and expected response signals 16a, 16b, 16c, hereinafter termed "setpoint response," step 104. Thereafter, the microprocessor raises counter A by 1, step 106. Subsequently, microprocessor 13 initiates the transmission of a search signal by transmitting/receiving device 11, step 108. The search signal, in addition to start- and synchronization information, contains, in particular, serial number 15 stored in memory 14. The search signal, advantageously, is unencrypted and is received by all remote control operations 20 located within the transmission range of signal transmission link 30 through their transmitting/receiving devices 21.

Their microprocessors 23, upon receiving a search signal, test whether serial number 15 transmitted along with the search signal agrees with the serial number functioning as reference signal and stored in memory 24 of remote control operation 20. In the case of non-agreement, remote control operation 20 does not participate further in the matching test. In the event of agreement between the signals compared with each other, microprocessor 23 brings about a response in the form of a contact signal, step 112. Functioning as contact signal is a short, simply constructed signal, for example group number 25 of respective remote control operation 20 in bit-coded form. It is advantageous if the contact signal, like the search signal, is unencrypted. The transmission of the contact signal is effected by microprocessor 24 after the expiration of a time interval from the reception of the search signal, the time interval being determined by group number 25 and being characteristic for remote control operation 20. The transmission then takes place in a time window having predetermined length. The transmission is dimensioned such that a reliable assignment of the contact signal to the time window is possible both for remote control operation 20 as well as for base station 10.

By checking the time windows in which the contact signals have been received, microprocessor 13 of base station 10 then establishes which remote control operations 20 having which group numbers are present, step 114. If no remote control operation 20 is detected as being present, microprocessor 13 checks the value of counter A, step 116. If it is

smaller than a predetermined reference value, for example 5, the microprocessor immediately once again causes the transmission of a search signal and repeats the process from step 106 in sequence. If the reference value is exceeded, microprocessor 13 interrupts the matching test, step 117. If the check test in step 114 yielded the result that at least one remote control operation 20 is present, microprocessor 13, from among present remote control operations 20, selects one, using which it subsequently carries out a matching test, step 118. After selecting a remote control operation, it sets a second internal counter B up one level, step 120. Thereafter, microprocessor 13 causes the transmission of a subsequent challenge signal via transmitting/receiving device 11. Random number 18, stored in memory 14, functions as the challenge signal.

Selected remote control operation 20, through its transmitting/receiving device 21, receives the challenge signal and from it, in connection with manufacturer code 27 and encryption keycode 31, formulates a "response" signal, which the remote control operation returns to base station 10 as the responding signal, step 124.

Microprocessor 13 of base station 10 compares for content the response signal sent back by remote control operation 20 with setpoint response signals 16a, 16b, 16c, previously loaded in step 104, of selected remote control operation 20, step 126. If the setpoint response signal and the response signal agree, microprocessor 13 sets internal counter B back to value 0, step 132, and it causes the transmission of a release signal, which, for example, makes possible the access to a motor vehicle and/or its operation, step 134. Subsequently, microprocessor 13 determines a random number 18 and, for every group number 25 entered in directory 16, establishes a new setpoint response signal, step 136. Using random number 18 and the newly formed setpoint response signals, the microprocessor then once again occupies memory locations 16a, 16b, 16c, and 18. The new memory contents function as the basis for the assignment test in connection with the next renewed triggering process. In rewriting memory contents 16 and 18, the matching test process is terminated, step 138.

If the check test in step 126 yields the result that the response signal sent back from remote control operation 20 does not agree with setpoint response signal 16a, 16b, 16c, loaded from the processor, microprocessor 13 sets internal counter B higher by one level, step 128. It then checks as to whether the contents of counter B exceed a prescribed limit value, for example,

the value 3, step 130. If that is the case, microprocessor 13, in accordance with step 136, establishes a new random number 18 and new setpoint response signals 16a, 16b, 16c, using which it overwrites the corresponding memory contents in memory 14. Then it terminates the assignment test process, step 138.

If the check test in step 130 yields the result that the limit value assigned to counter B has not yet been exceeded, microprocessor 13 also carries out a redetermination of random number 18 and of setpoint response signals 16a, 16b, 16c, in accordance with step 136. Subsequently, however, it continues in the repetition of step 104 and immediately reloads the redefined memory contents 18 and 16a, 16b, 16c, to carry out subsequent step 106.

Provision can be made to carry out the determination of a new random number and a new setpoint response signal in accordance with step 136 in a controlled and deliberate manner. Since the redetermination takes place only in response to an authorized use in connection with the confirmation of matching and of the transmission of a release signal, a deliberate execution of step 136 does not have an impact for the authorized user. On the contrary, it is made more difficult for an unauthorized user to simulate a matching of a remote control operation to a base station, even if it should be possible to cause the base station to transmit the challenge signal to the remote control operation by simulating a contact signal. Through a controlled lengthening of the time for carrying out step 136, it is also made more difficult to discover a correct response signal through a permutative repetition of possible response signals.